Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

Forensics Investigation Report

A. Objective

a. To determine if Wadith "Paul" Nader possessed child pornography.

B. Search Authority

a. On March 16, 2015, Detective Bryan Svajgl obtained a search warrant signed by the Honorable Judge Hutton of the Sarpy County Court authorizing the search of numerous types of electronic devices and media obtained from the residence at 912 Hickory Hill Road in Papillion, Nebraska.

C. Evidence Analyzed

a. HP Envy, Model: 15-J053CL, SN: 6CG3180RF (Lab reference no: 2015-27-1-1)
   750 GB Seagate Momentus, Model: ST750LX003, SN: W200BJB9 (Lab reference no: 2015-27-1-1-HD1)
b. 2TB Seagate Barracuda Green, Model: ST2000DL003, SN: 6YD0D6MX (Lab reference no: 2015-27-1-HD1)
   Contained in a silver and black HDD Enclosure, Model: WLX 393 U3
c. Samsung Galaxy S4, Model: SGH-I337, SN: R31D50L504P (Lab reference no: 2015-27-1-2)
   64GB SanDisk Ultra Micro SD card, SN: 4302PM00T29E (Lab reference no: 2015-27-1-2-SD1)
d. HP Pavilion, Model: dv7-6168nr, SN: 5CH13513SM (Lab reference no: 2015-27-1-3)
   1TB Toshiba, Model: MQ01ABD100, SN: 134GS3U1S (Lab reference no: 2015-27-1-3-HD1)
   1TB Samsung Spinpoint, Model: ST1000LM024, SN: S2Y9J9DD300808 (Lab reference no: 2015-27-1-3-HD2)
e. Files obtained from Microsoft for the wadith@hotmail.com account. (Lab reference no: 2015-27-2-1)
f. ASUS Transformer, Model: T100T, SN: E8N0BCIRR07D34D (Lab reference no: 2015-27-1-4)

D. Processing

a. To protect the integrity of the data contained on all fixed and removable media, all information was copied to another storage media where a sector-by-sector image is created. The acquired image is called an "Evidence File". Throughout the creation of this "Evidence File" the image is continually verified by both a CRC (Cyclical Redundancy Check) value for every 32K block, as well as an MD5 hash calculated for all data contained in the "Evidence File". Both the CRC and MD5 hash values are immediately assigned to the "Evidence File" upon acquisition. This process not only copies all the standard DOS and Windows compatible files, but it also copies all file slack, erased files and unallocated space. This procedure does not affect, change or alter the information on the original storage media in any manner.

E. Acquisition

a. **2015-27-1-1 - HP Envy, Model: 15-J053CL, SN: 6CG3180RF**
   An examination of the laptop revealed no visible damage. I photographed the device and labeled it lab reference number 2015-27-1-1. I removed a panel on the bottom of the laptop and observed one hard drive. Once removed the drive was examined with no visible damage found, photographed and labeled 2015-27-1-1-HD1.

   At this point, I would normally boot the laptop and observed the date and time in the BIOS setup. The laptop was brought into the lab without its power adapter and would not boot via the battery. I contacted Det. Svajgl via email and inquired if he could provide this power adapter.

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

On 5/29/15, Det. Svajgl delivered the power adapter to the lab. With the hard drive removed, I checked the time and date of the laptop by hitting the F10 key after powering the device on to enter the BIOS setup. The time and date showed as 05/29/2015 at 11:06:02. I compared this with the time and date for Central Time using the NIST date/time website (http://time.gov/HTML5/) and appeared as 05/29/2015 at 11:06:01.

2015-27-1-1-HD1 - 750 GB Seagate Momentus, Model: ST750LX003, SN: W200BJB9
I connected the drive labeled 2015-27-1-1-HD1 to a forensic workstation via a Tableau Forensic SATA Bridge write blocker, SN 5535904F and obtained pre-acquisition MD5 and SHA-1 hash values using FTK Imager. Once this process completed, I acquired a forensic evidence file of the drive using FTK Imager. A case folder, 2015-27, was created on the TCL network storage server and the forensic evidence file stored in this folder. FTK Imager performs MD5 and SHA-1 hash analysis of the drive after acquisition. These values were identical to the pre-acquisition hash values.

b. **2015-27-1-HD1 - 2TB Seagate Barracuda Green, Model: ST2000DL003, SN: 6YD0D6MX**
An examination of the HDD enclosure revealed no visible damage. I photographed the device and labeled it lab reference number 2015-27-1-HD1. I removed 3 screws from one of the side panels. The fourth screw was stripped, but I was able to slide the panel aside to access the hard drive. I observed one hard drive and a folded piece of paper within the enclosure. The single sheet of paper was blank. I removed the drive by sliding it away from the logic board and lifting it out. Once removed, the drive was examined with no visible damage found, photographed and labeled 2015-27-1-HD1.

I connected the drive labeled 2015-27-1-HD1 to a forensic workstation via a Tableau Forensic SATA Bridge write blocker, SN 5535904F and obtained pre-acquisition MD5 and SHA-1 hash values using FTK Imager. Once this process completed, I acquired a forensic evidence file of the drive using FTK Imager. The forensic evidence file was stored in case folder, 2015-27, located on the TCL network storage server. FTK Imager performs MD5 and SHA-1 hash analysis of the drive after acquisition. These values were identical to the pre-acquisition hash values

c. **2015-27-1-2 - Samsung Galaxy S4, Model: SGH-I337, SN: R31D50L504P**
I removed the cell phone from the evidence bag and observed it to be in an Otterbox protective case. It appears the back of the case had been opened prior to submission into the lab. I removed the phone from the protective case and performed an inspection which revealed no visible damage. I photographed the device both in and out of the case and labeled it lab reference number 2015-27-1-2. I removed the back cover of the phone and observed one Micro SD card and one SIM card. I removed the Micro SD card so I could process it separately. I placed the phone in an EDEC shielding bag to prevent it from establishing a connection to any network. I then connected the phone to the wall charger and powered on the device and observed it to be in "Airplane Mode", which prevents the phone from connecting to a network. The phone did not require a lock code or password for access. I removed the device from the shielding bag and allowed it to fully charge.

Once charged, I attempted to obtain a physical image using Cellebrite UFED Touch by selecting the Samsung SGH-I337M option on the UFED Touch, selected "Physical Extraction". I was presented with the instructions uncheck the "Verify Apps" box under "Settings", "More" and "Security" and enable "USB Debugging" under "Settings", "More", "Developer Options". I navigated to both areas and found both to be in the desired state. I exited "Settings" by pressing the Home button to go back to the Home screen and proceeded to exempt the extraction but was unable to do so because the phone was not

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

rooted. I was presented with the option to obtain a backup of the device via the File System Extraction option. I elected to abort the Physical extraction operation.

I then reselected the Samsung SGH-I337M option on the UFED Touch, selected "File System Extraction" and "Android Backup". I was presented with the same instructions as above, as well as, additional instructions to uncheck the "Stay Awake" and "Verify Apps via USB" boxes. Both located under "Settings", "More", "Developer Options". I found both to be in the desired state. I exited "Settings" by pressing the Home button to go back to the Home screen and proceeded with the extraction. Once the extraction was complete, I generated a report including a timeline using Physical Analyzer.

2015-27-1-2-SD1 - 64GB SanDisk Ultra Micro SD card, SN: 4302PM00T29E
An examination of the SD card revealed no damage and, due to space constraints, was labeled SD1. I used the lab's Transcend Micro SD Adapter P3-081511, SN P00600 and a Tableau T8 USB write blocker, SN T005A016620 to obtain pre-acquisition MD5 and SHA-1 hash values using FTK Imager. Once this process completed, I acquired a forensic evidence file of the drive using FTK Imager. The forensic evidence file was then stored in in case folder, 2015-27, located on the TCL network storage server. FTK Imager performs MD5 and SHA-1 hash analysis of the drive after acquisition. These values were identical to the pre-acquisition hash values.

d. **2015-27-1-3 - HP Pavilion, Model: dv7-6168nr, SN: 5CH13513SM**
An examination of the laptop revealed no visible damage. When I lifted the lid, I observed a green sticky note underneath the keyboard with various notations including "Nikkl1973 --> Passwd". I photographed the device and labeled it lab reference number 2015-27-1-3. I removed a panel on the bottom of the laptop and observed two hard drives. Once removed each drive was examined revealing no visible damage, photographed and labeled 2015-27-1-3-HD1 and 2015-27-1-3-HD2, respectively.

With the hard drives removed, I checked the time and date of the laptop by hitting the Esc key and then the F10 key after powering the device on to enter the BIOS setup. The time and date showed as 06/11/2015 at 14:02:02. I compared this with the time and date for Central Time using the NIST date/time website (http://time.gov/HTML5/) and appeared as 06/11/2015 at 14:00:11.

2015-27-1-3-HD1 - 1TB Toshiba, Model: MQ01ABD100, SN: 134GS3U1S
I connected the drive labeled 2015-27-1-3-HD1 to a forensic workstation via a Tableau Forensic SATA Bridge write blocker, SN 5535904F and obtained pre-acquisition MD5 and SHA-1 hash values using FTK Imager. Once this process completed, I acquired a forensic evidence file of the drive using FTK Imager. The forensic evidence file was stored in case folder, 2015-27, located on the TCL network storage server. FTK Imager performs MD5 and SHA-1 hash analysis of the drive after acquisition. These values were identical to the pre-acquisition hash values.

2015-27-1-3-HD2 - Samsung Spinpoint, Model: ST1000LM024, SN: S2Y9J9DD300808
I connected the drive labeled 2015-27-1-3-HD2 to a forensic workstation via a Tableau Forensic SATA Bridge write blocker, SN 5535904F and obtained pre-acquisition MD5 and SHA-1 hash values using FTK Imager. Once this process completed, I acquired a forensic evidence file of the drive using FTK Imager. The forensic evidence file was stored in case folder, 2015-27, located on the TCL network storage server. FTK Imager performs MD5 and SHA-1 hash analysis of the drive after acquisition. These values were identical to the pre-acquisition hash values.

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

e. **2015-27-2-1 - Files obtained from Microsoft for the wadith@hotmail.com account**
The Technical Crimes Lab (TCL) received an external hard drive from Det. Svajgl containing 13 .zip files obtained from Microsoft pursuant to a search warrant on user account, wadith@hotmail.com. Between 7/13 and 7/15, I unzipped each of the .zip. I found that I could not extract file, GCC-657624-Y9D4Z0_07_14 as it was corrupted. I attempted to download the file using information I had obtained from Det. Svajgl but was unable to do so as the time frame for download had expired. The Detective contacted Microsoft and provided me with valid download links and I was able to successfully download and extract the file on 7/28.

f. **2015-27-1-4 - ASUS Transformer, Model: T100T, SN: E8N0BCIRR07D34D**
An examination of the device revealed no visible damage. I attempted to enter BIOS by hitting F2 on the keyboard but the device booted through to the Windows 8.1 logon screen. The account that appeared on the logon screen was Raiyah Nader, raiyah.noor1@gmail.com. I attempted to enter the BIOS again by holding the down volume button while powering on the tablet. I was able to enter BIOS and disable the Secure Boot option. I then attempt to boot Paladin from an external drive and a USB key without success. I re-enabled Secure Boot, powered the device off and returned it to the evidence room.

F. **Analysis**

1. **2015-27-1-3-HD2 - HP Pavilion, Model: dv7-6168nr, SN: 5CH13513SM**

a. **Images and Video**

i. I processed forensic evidence file using NetClean Analyze DI to recover images and video. NetClean compares hash values as well as utilizing visual matching technology called PhotoDNA of known child pornography and categorizes those files as such thus filtering them from unknown images and videos. A hash value is a unique identifier or a digital fingerprint generated by an algorithmic calculation that is determined by the file's content which will remain the same value even if the file has been renamed. NetClean utilizes hash and PhotoDNA databases obtained from Project Vic. Project Vic is an ecosystem of information for the purpose of data sharing between worldwide law enforcement agencies to standardize classification of images and videos depicting known child pornography.

I searched for the same filenames as submitted via the Cybertips #3184694 and #3320099 which produced 4 hits. I classified images "1773334201.jpg", "409277812.jpg" and "1600471024.jpg" as in violation of statute §28-813.01. The females depicted in these images appear to be approximately 12-14 years of age. It should be noted that prior to the submission of this case to the NSP TCL, Det. Svajgl submitted the 7 images that were uploaded to Skydrive to the Child Victim Identification Program (CVIP) for review. According to CVIP report #84278, images "1773334201.jpg" and "409277812.jpg" contain child victims who have been identified by law enforcement as the "Blue Pillow" series and the "Colorful Bedroom" series, respectively. The image named, "1766201396.jpg", was classified as Age Difficult as it depicts a female who appears to be approximately 14-18 years of age. While all of these images were located the Recycle Bin, all were previously located in the "arely" folder of the Administrator user account.

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

I performed a visual examination of the remaining images and videos and classified 3 additional images as in violation of state statute §28-813.01. Hash values for the images were submitted to the National Center for Missing and Exploited children (NCMEC) for possible matches to a child or children previously identified by law enforcement. The NCMEC report can be found in the "NCMEC" section of this report.

The image file named "368391694.jpg" depicts a nude female who appears to be 11-14 years of age posing in front of a bathroom mirror with her panties pulled down to expose her vagina. She is holding what appears to be a cell phone as if she is taking a picture of herself. The female has underdeveloped breasts and no apparently developing pubic hair. Per NCMEC, this image depicts a child victim who has been identified by Law Enforcement. A visually similar, duplicate image named, "1894962318.jpg" was also located. While these images were located the Recycle Bin, they were previously located in the "arely" folder of the Administrator user account.

The image file named "219432669.jpg" depicts a topless female who appears to be 12-14 years of age posing in front of a mirror in purple panties. She is holding a camera as if she is taking a picture of herself. The female has small, developing breasts and developing hips. Per NCMEC, this image depicts a child victim who has been identified by Law Enforcement. While this image was located the Recycle Bin, it was previously located in the "arely" folder of the Administrator user account.

The image file named "265198495.jpg" depicts a nude female who appears to be 11-14 years of age lying on a bed with her legs spread exposing her vagina. She has underdeveloped breasts, developing hips and some pubic hair. Per NCMEC, this image has not been identified by Law Enforcement. While this image was located the Recycle Bin, it was previously located in the "Hot N Hairy" folder of the Administrator user account.

146 unique images were classified as Age Difficult. The images depict age difficult females in various states of dress including nude and engaging in sexual situations. None of the images came back as identified by Law Enforcement. All but 2 of the above cited images in this section were located in the in the Recycle Bin of the Administrator user account.

b. Windows Artifacts

I performed a search for c:\Other in X-Ways. I received many text hits including filenames "1773334201.jpg", "409277812.jpg", "1600471024.jpg", and "1766201396.jpg" the WetTransferInfo.dat file. This log file was the same size and had the same creation date of 12/09/2013 as the WetTransferInfo.dat file located on evidence item 2015-27-1-1-HD1. Please see section E. 2. c. ii below.

2. 2015-27-1-1-HD1 - HP Envy, Model: 15-J053CL, SN: 6CG3180RF

a. System Information and Time Zone Determination

i. I used X-Ways to copy out necessary registry hives and ntuser.dat files and examined them using Registry Browser. The computer name was PAULS and last shutdown date was 3/16/2015 at 22:22 hours. The machine was running Windows 8.1 with the registered owner being wadith@hotmail.com. There was one user created account called Paul.

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

ii. From this, I discovered that the active time bias was set to Central Daylight Time or -5 hours from GMT. I then entered this time zone into X-Ways, Internet Evidence Finder (IEF) and EnCase, so it could adjust dates and times to display them as the user would have seen them.

b. Search History

i. I used Internet Evidence Finder (IEF) to extract keywords and phrases used to conduct internet searches. Please see the Internet Related section of this report.

a. Google Searches: Searches conducted using Google in Firefox:
12/21/14: "how to delete onedrive"
12/22/14: "how to move e-mail from hotmail to gmail on my phone"
12/22/14: "transfer all data from hotmail to gmail using smart phone"
1/28/25: "hairy black haired teen porn", "hairy black haired teen porn beautiful", "hairy black haired teen porn beautiful mexico", "hairy teen porn beautiful", "hairy teen porn beautiful 3 some", "hottest teen porn"
2/22/15: "tor" - NOTE: no instance of Tor was located on the laptop
3/10/15: "teen squirts more than I have ever seen"

b. Parsed Search Queries: Searches conducted using Bing and Bing Videos in Firefox and Opera Browsers:
9/16/14: "young Drug Addict Porn", "young junkie sex"
10/10/14: "teenage seductress", "teenage seductress 1971"
10/14/14: "family fun"porn", "family fun"porn in 1970", "family fun"porn in 1980s", "family fun"porn classic"
11/10/15: "High School Girls Locker Room", "High School Locker Room"
11/17/14: "hairy tiny tits threesome", "Tiny Preteebn Puffy Tits"
11/19/14: "teenage cookies", "teenage cookies vporn"
11/24/14: "cherry hill high porn", "cherry hill porn"
*1/1/15: "Rainbow party", "Rainbow party blowjob", "Rainbow party Lipstick Rings", "Rainbow parties High School", "Teen Rainbow Party"
* I performed a Google search for "Rainbow Party" and located the following definition according to Wikipedia. "A variant of other sex party urban myths, the stories claim that at these events, allegedly increasingly popular among adolescents, females wearing various shades of lipstick take turns fellating males in sequence, leaving multiple colors (a "rainbow") on their penises."
1/14/15: "Little Tiny Titted Girls"
1/19/15: "MILF stepmom threesome with teen couple"
1/26/14: "Hidden Teen Shower"
1/28/15: "hairy teen porn beautiful 3 some", "hairy teen porn beautiful 3 SOME", "hottest teen porn", "hottest teen porn pale", "teen 4 some"

c. Windows Artifacts

i. I performed a keyword search using the filenames of all the images submitted via Cybertips selecting all artifacts recovered from Firefox, Internet Explorer, Chrome and Opera. This search resulted in one hit in Internet Explorer in the WebCacheV01.dat file. It should be noted that history recovered from this file includes both visited webpages and files accessed on the computer via File Explorer. On 5/6/14, user "Paul" accessed a file named "1850260232.jpg" located at C:\Other\arely. Since the root of the C:\ is not the Windows

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

default location for saving and storing pictures, I navigated to C:\Other in X-Ways and observed 166 uniquely named folders collectively containing a large amount of various types of pornographic images and videos. A file by this name was no longer located in C:\Other\arely nor did I observe any image that was visually similar to the image that was submitted in the Cybertip.

ii. I performed a search for c:\Other in X-Ways. I received many text hits including filenames "1773334201.jpg", "409277812.jpg", "1600471024.jpg", and "1766201396.jpg" from a file called WetTransferInfo.dat with a creation date of 12/09/2013. I performed a Google search and learned that this is a log of files transferred when a user runs the Windows Easy Transfer feature. This feature guides a user through the process of transferring files and settings from one computer to another. I performed a test of the Windows Easy Transfer (WET) feature and learned that the WetTransferInfo.dat is created each time a user transfers files to a computer using this tool. The .dat file is created in a folder that reflects the date of the transfer, the creation date of the .dat reflects the date/time the transfer was started and the modified date reflects the date/time the transfer completed. Each time the WET process is run, a new folder is created at \ProgramData\Microsoft\Windows Easy Transfer\PostMigData\. There were six folders in this directory dating from 12/5 to 12/10/13. The WetTransferInfo.dat file that lists these hits were located in folder "2013-12-10" with a created date of 12/9/2013 at 23:47 and modified date of 12/10/13 at 08:06. Based on these test results, it appears the above named files existed on the machine as of 12/09-10/2013.

I created a report of the WetTransferInfo.dat file located in folder 2013-12-10 using Windows Easy Transfer Reports tool in a Windows 7 virtual machine. I copied out the 2013-12-10 folder using X-Ways to the TCL storage server then copied the folder to C:\ProgramData\Microsoft\Windows Easy Transfer\PostMigData\ to the virtual machine and proceeded to create the report. This report shows the filename, location on old PC and location on new PC. A total of 157,432 files were transferred with 47,618 of those files being copied to C:\Other and 2,905 of those files being copied to C:\Other\arely. At the time of the transfer, there were 36 folders located in C:\Other\arely to include notable folder names listed below. This total does not include folders created within these subfolders. An Excel spreadsheet of the transferred files can be found in the Windows Artifacts section of this report.

- "01 Hairy Teens"
- "1 Awesome Teen Ass Fuckin"
- "1.7 Hot Juciy gooey self shot Teen"
- "2.0 awesome hairy Spanish teen"
- "Awesome French Teens"
- "Cute Curly Teen"
- "Cute Teenie Bopper"
- "Hot French Teen"
- "Hot hairy teen shaving"
- "Hot Teenie Self Shot"
- "Maine Teen"
- "Tiny Titted Hairy Crazy Czech"

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

Next, I navigated to C:\Other\arely on the forensic evidence file of the laptop and noted that number of files that existed in this folder at the time the laptop was seized to be 291 including two subfolders. The creation dates of these files are between 1/1/15 and 3/10/15. None of the folders transferred in 2013 existed at this location at the time the laptop was seized. I performed a search of filenames, all having a .jpg extension, that were transferred to this folder in 2013. This search produced zero hits.

d. Images and Video

i. I processed forensic evidence file using NetClean Analyze DI to recover images and video from the digital media. The evidence was processed utilizing Project Vic databases, as well as, databases I created based on my examination of evidence item 2015-27-1-3-HD2. I also performed a text search for the filenames of the images submitted via the Cybertips, which produced no hits.

I performed a visual examination of the remaining images and videos and classified 3 additional images as in violation of state statute §28-813.01. Hash values for the images were submitted to the National Center for Missing and Exploited children (NCMEC) for possible matches to a child or children previously identified by law enforcement. The results are shown below. The NCMEC report can be found in the "NCMEC" section of this report.

The image file named "405401360.jpg" depicts a nude female who appears to be 12-14 years of age sitting outdoors with her legs closed and displaying her underdeveloped breasts. This image was located at "Other\arely" and "Other\Awesome". Per NCMEC, this image has not been identified by Law Enforcement.

The image file named "656469771.jpg" depicts a nude female who appears to be 12-14 years of age standing outdoors. The female has underdeveloped breasts and no apparently developing pubic hair. This image was located at "Other\arely". Per NCMEC, this image has not been identified by Law Enforcement.

The image file named "772074859.jpg" depicts a female who appears to be 12-14 years of age wearing only a pink skirt lying on a bed with colored pillows. Her legs spread exposing her vagina. She has underdeveloped breasts, developing hips and some pubic hair. This image was located at "Other\arely". Per NCMEC, this image has not been identified by Law Enforcement.

111 images and 1 video were classified as Age Difficult. The images depict age difficult females in various states of dress including nude and engaging in sexual situations. None of the files came back as identified by Law Enforcement.

3. 2015-27-2-1 - Files obtained from Microsoft for the wadith@hotmail.com account

a. Images

i. Using EnCase 7, I created a case called Microsoft Search Warrant on the TCL network server. I added each of the folders to the case and performed pre-processing including a keyword search for "1773334201.jpg", "1850260232.jpg", "409277812.jpg", "829555945.jpg", "864858517.jpg", "1600471024.jpg" and "1766201396.jpg". This produced hits on all 7 images being located at "Documents\Other\arely" in Skydrive. The path, "Other\arely", is consistent with the location files with the same name were stored on the HP Envy laptop

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

(lab reference number 2015-27-1-1-HD1) and on the HP Pavilion laptop (lab reference number 2015-27-1-3-HD2). Also located in "Documents\Other\arely", "368391694.jpg", "1894962318.jpg" and "219432669.jpg" that depicted children previously identified by Law Enforcement. These images were also located on the HP Pavilion laptop (lab reference number 2015-27-1-3-HD2). Please see section E. 1. b. i.

b. Email

i. The above mentioned search produced no hits associated with any emails obtained from the account. Additionally, I reviewed emails provided by Microsoft and found nothing of investigative interest.

4. **2015-27-1-HD1 - 2TB Seagate Barracuda Green, Model: ST2000DL003, SN: 6YD0D6MX**
   i. I processed forensic evidence file using NetClean Analyze DI utilizing Project Vic databases, as well as, databases I created based on my examination of evidence item 2015-27-1-3-HD2. I also searched for the filenames of the images submitted in the Cybertips, as well as, the filenames of the images depicting identified children. This produced no hits.

   Processing produced approximately 15 hits from files in the Age Difficult category. There were approximately 1.6 million files that were uncategorized. I performed a less extensive preview search of approximately 60,000 files and observed a large amount of pornography, much like with the two laptops I had already examined. As such, I elected not to perform an extensive visual search.

5. **2015-27-1-2 - Samsung Galaxy S4, Model: SGH-I337, SN: R31D50L504P**
   2015-27-1-2-SD1 - 64GB SanDisk Ultra Micro SD card, SN: 4302PM00T29E
   i. Nothing of investigative interest was located on either device.

6. **2015-27-1-3-HD1 - HP Pavilion, Model: dv7-6168nr, SN: 5CH13513SM**
   i. Nothing of investigative interest was located.

7. **2015-27-1-4 - ASUS Transformer, Model: T100T, SN: E8N0BCIRR07D34D**
   i. I was unable to obtain an acquisition of the device. The account that appeared on the logon screen was Raiyah Nader, raiyah.noor1@gmail.com.

G. CVIP Submission

a. A disc of images and videos located in this examination will be sent to their CVIP (Child Victim Identification Program) for manual review. This will give a more accurate count of how many images and videos actually contain child victims. Additionally, this will give law enforcement contact information of the originating agency that discovered the victim, allowing additional verification. For some victims, victim impact statements may be obtainable.

Nebraska State Patrol Technical Crimes Unit
An Internet Crimes Against Children Task Force
3800 NW 12th Street. Lincoln, NE 68521
Phone: (402) 479-4916 Fax: (402) 479-4950

H. Certification

a. I hereby certify that, unless stated otherwise, the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

Shelby Mertins

Digitally signed by Shelby Mertins
DN: cn=Shelby Mertins, o=Nebraska State Patrol, ou=Technical Crimes/ICAC, email=shelby.mertins@nebraska.gov, c=US
Date: 2015.08.19 14:32:24 -05'00'

1. Appendix A : Programs Used

i. Operating Systems
   a. Windows 8.1 Pro
   b. Windows 7 Ultimate SP1

ii. Windows Forensic Programs
   a. EnCase 7.09
   b. X-Ways 18
   c. Internet Evidence Finder 6.6
   d. Registry Browser 3
   e. NetClean Analyze DI 15.2
   f. FTK Imager 3.1.4.6

iii. Other Programs
   a. Microsoft Office 2010
   b. Notepad++ 5.9.3
   c. VMWare Workstation 10

Date/Time Recovered: 3-17-15 1107

Page 1 of 1

LA VISTA POLICE
7701 SOUTH 96TH STREET
EVIDENCE/PROPERTY REPORT

IR # 15-5282

CONTROL #

LOCATION PROPERTY SEIZED/RECOVERED: 912 Hickory Hill Rd Papillion NE

Offense: Possession of child pornography

CODE: ENTER ALL THAT APPLY IF KNOWN CODES: O-OWNER V-VICTIM S-SUSPECT F-FOUND BY D-DEPARTMENT ☐ OWNER UNKNOWN

1. NAME LAST Nader FIRST Wadith MIDDLE
ADDRESS 912 Hickory Hill Rd Papillion PHONE

2. NAME LAST FIRST MIDDLE
ADDRESS PHONE

3. NAME LAST FIRST MIDDLE
ADDRESS PHONE

4. NAME LAST FIRST MIDDLE
ADDRESS PHONE

☒ FELONY ☐ MISDEMEANOR

PROPERTY SHOULD BE:
☒ Kept as evidence
☐ Safekeeping
☐ Destroyed
☐ Released
☐ Found Property

RELEASED TO:
☐ Owner
☐ Other

Results Of ☐ Search ☐ Other
☐ Arrest ☒ Recovered ☐ Found

Item	Quantity	Description	Code	Model/Serial #	Released To:
01	1	DVD+R containing ostiage report	D	—	

Submitting Officer/ID #	Date/Time Submitted	Locker #	Evidence Tech. Receiving	Date/Time Received	Storage Location
B. Iversen 15051	0949 3-30-15	Evidence Tech			

Disposition of Property | Date | By | ID#

County Attorney Case Disposition

☐ Release Marked Items to Owner
☐ Destroy Marked Items
C/A Signature: Date:

4/05 WHITE-ORIGINAL YELLOW-RECORDS PINK-PROPERTY GOLD-RECEIPT